

Implementation Guide

Novell[®] Sungard Banner Driver

4.0.1

January 17, 2012

www.novell.com



Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. For more information on exporting Novell software, see the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/). Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see [Novell Documentation \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/).

Novell Trademarks

For a list of Novell trademarks, see [Trademarks \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	5
1 Overview	7
1.1 Introduction	7
1.2 How the Driver Works	7
1.3 Key Driver Features	8
1.3.1 Local Platforms	8
1.3.2 Remote Platforms	8
1.3.3 Supported Operations	8
1.3.4 Password Synchronization Support	9
2 Installing the Sungard Banner Driver	11
2.1 Getting the .iso File from the Novell Download Site	11
2.2 New Installation by Using Physical Media or ISO	12
3 Creating a Working Driver	13
3.1 Creating the Driver in Designer	13
3.1.1 Installing the Current Driver Packages	13
3.1.2 Installing the Driver	14
3.1.3 Configuring the Driver	17
3.1.4 Configuring Driver Parameters	17
3.1.5 Deploying the Driver	18
3.1.6 Extending the Schema	19
3.1.7 Understanding Institutional Roles	20
3.1.8 Starting the Driver	21
3.2 Activating the Driver	22
3.3 Sungard Banner Requirements	22
4 Customizing the Driver	23
4.1 Managing the Driver	23
4.2 Schema Mapping	23
4.2.1 User Attributes Mapping	23
A Driver Properties	27
A.1 Driver Configuration	27
A.1.1 Driver Module	27
A.1.2 Driver Object Password	28
A.1.3 Authentication	28
A.1.4 Startup Option	29
A.1.5 Driver Parameters	30
A.2 Global Configuration Values	31
A.3 Extension Attributes	33

B	Securing the Driver	35
B.1	Configuring the Publisher Channel	35
B.2	Configuring the Subscriber Channel	36

About This Guide

This guide explains how to install and configure the Novell Identity Manager 4.0.1 Sungard Banner driver.

This guide contains the following sections:

- ♦ [Chapter 1, “Overview,” on page 7](#)
- ♦ [Chapter 2, “Installing the Sungard Banner Driver,” on page 11](#)
- ♦ [Chapter 3, “Creating a Working Driver,” on page 13](#)
- ♦ [Chapter 4, “Customizing the Driver,” on page 23](#)
- ♦ [Appendix A, “Driver Properties,” on page 27](#)

Audience

This guide is intended for consultants and administrators implementing the Novell Identity Manager driver for Sungard Banner. You should have an understanding of the Sungard Banner system, SPML, SOAP, and HTML.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Identity Manager Sungard Banner Guide*, visit the [Identity Manager Documentation Web site](http://www.novell.com/documentation/idm401drivers/) (<http://www.novell.com/documentation/idm401drivers/>).

Additional Documentation

For documentation on other Identity Manager drivers, see the [Identity Manager Documentation Web site](http://www.novell.com/documentation/lg/dirxmldrivers/index.html) (<http://www.novell.com/documentation/lg/dirxmldrivers/index.html>).

Overview

1

- ♦ Section 1.1, “Introduction,” on page 7
- ♦ Section 1.2, “How the Driver Works,” on page 7
- ♦ Section 1.3, “Key Driver Features,” on page 8

1.1 Introduction

The Novell Identity Manager driver for Sungard Banner integrates with the Sungard Banner system. The driver synchronizes identity information for students, faculty and staff in the higher education environment. This information is stored in the Identity Vault where it can be synchronized with other applications.

Sungard Banner provides the Unified Digital Campus to unify people, processes, and technology in an environment that addresses the needs of higher education institutions and the people they serve. The Sungard Banner solutions involve the Banner Suite, Luminis Portal, and Workflow and other applications. Although the architecture of the Sungard Banner driver and the Sungard Banner data interfaces the driver uses are intended to allow a single driver to integrate with any of the Sungard components, version 4.0.1 of the driver only supports the Banner Suite.

Sungard Banner communicates identity information by using the UDCIdentity schema in SPML 2.0 formatted documents. The Identity Manager driver for Sungard Banner converts the UDCIdentity schema from SPML 2.0 format into Novell XDS format and publishes the resulting document to the Identity Vault.

For more information about the UDCIdentity, see the *Sungard Banner Identity Handbook*.

For more information on SPML 2.0, see <OpenSMPL.org> (<http://www.openspml.org/>).

1.2 How the Driver Works

The Identity Vault uses XDS, a specialized form of XML, to represent events in the Identity Vault. The Novell Identity Manager passes the XDS to the driver policy, which can consist of basic policies, DirXML Script, and the XSLT style sheets.

The following diagram illustrates the data flow between the Identity Manager and the Sungard Web service:

Figure 1-1 *Sungard Banner Driver Data Flow*



The schema mapping driver policy translates the Identity Vault Schema in XDS to UDCIdentity.

The Subscriber channel of the driver shim receives the XML from the driver policy and converts the UDCIdentity data from XDS format into SPML 2.0 format. The driver then encapsulates the SPML in a SOAP envelope and uses HTTP to communicate with the Web service. The hand-off between the driver shim and the application is serialized XML.

The Web service or application processes the request and returns a SOAP response to the driver shim. The shim receives the response as an array of bytes and converts it to an SPML document before passing it back to the driver policies. The Novell Identity Manager driver for Sungard Banner processes the response, converting it into XDS that is reported back to the Identity Vault.

The Publisher channel of the driver shim receives a UDCIdentity in SPML from Banner Enterprise Identity Services (BEIS) and converts the UDCIdentity data into XDS format. The driver then passes the XDS to the Identity Manager engine, where the Schema Mapping policy converts the UDCIdentity into the eDirectory schema before committing the object to eDirectory.

Identity Manager processes the change and returns a response formatted in XDS. The driver converts the response into SPML and returns it to BEIS.

1.3 Key Driver Features

The following sections contain a list of the driver's key features:

- ♦ [Section 1.3.1, “Local Platforms,” on page 8](#)
- ♦ [Section 1.3.2, “Remote Platforms,” on page 8](#)
- ♦ [Section 1.3.3, “Supported Operations,” on page 8](#)
- ♦ [Section 1.3.4, “Password Synchronization Support,” on page 9](#)

1.3.1 Local Platforms

A local installation is an installation of the driver on the Metadirectory server. The Sungard Banner driver can be installed on the operating systems supported for the Metadirectory server.

For information about the operating systems supported for the Metadirectory server, see “[Metadirectory Server](#)” in “[System Requirements](#)” in the *Identity Manager 4.0 Framework Installation Guide*.

1.3.2 Remote Platforms

The Sungard Banner driver can use the Remote Loader service to run on a server other than the Metadirectory server. The Sungard Banner driver can be installed on the operating systems supported for the Remote Loader.

For information about the supported operating systems, see “[Remote Loader](#)” in “[System Requirements](#)” in the *Identity Manager 4.0 Framework Installation Guide*.

1.3.3 Supported Operations

The Sungard Banner driver interacts with Banner via Banner Enterprise Identity Services (BEIS). BEIS publishes data in SPML format. The driver is limited to operations supported by SPML. The basic configuration files for the Sungard Banner driver are capable of performing the following operations on User objects:

- ♦ Add
- ♦ Modify
- ♦ Delete

- ◆ Query
- ◆ Modify password

BEIS does not support rename or move operations. It is possible to synthesize these operations in an Identity Manager Policy based on attribute data changes in the XML data received from BEIS.

The driver publishes role information from the Sungard system. Roles are used to grant access to information on the Sungard Portal in Luminis and other Sungard applications and resources. Sungard does not delete identities after they are created. The Sungard system removes roles from the collection of roles on a given user. Consultants or Identity Manager administrators deploying the driver might implement Role-Based Entitlements on other drivers to react to changes in the list of roles for a given user.

For additional information, see [Section 3.1.7, “Understanding Institutional Roles,”](#) on page 20.

1.3.4 Password Synchronization Support

By default, the Novell Identity Manager driver for Sungard Banner policies do not synchronize passwords to or from the Sungard system. However, when a user is added to the Identity Vault, a password can be created for the user by selecting an attribute to pull the password from, or by generating a random password through a policy on the Publisher Channel Command Transform.

To configure this policy, set the *Banner Password Settings* attributes on the *Password Settings* tab of the GCV editor.

Select *Random Password* to have a random password generated for the new user. You can specify the number of alphabetic characters and numeric characters that must be used in generating the password.

Select *Attribute Value from User* to have a password value set from the value of an attribute on the user object. BEIS can be configured to publish a password from the Banner system as an extension attribute. The driver recognizes the extension attribute and publish it as an <add-attr> element in the XDS document to be sent to the Metadirectory engine. Map the Banner element name to an eDirectory attribute and set that attribute name as the *eDirectory attribute to use for initial password value* to have the driver password policy use the attribute in the specified eDirectory attribute as the user’s new password.

Installing the Sungard Banner Driver

2

The Sungard Banner driver can be installed on multiple systems and platforms. To verify the system requirement list, see “[System Requirements](#)” in the *Identity Manager 4.0 Framework Installation Guide*.

- ♦ “[Getting the .iso File from the Novell Download Site](#)” on page 11
- ♦ “[New Installation by Using Physical Media or ISO](#)” on page 12

2.1 Getting the .iso File from the Novell Download Site

- 1 Go to the [Novell Download page](http://download.novell.com) (<http://download.novell.com>).
- 2 In the *Product or Technology* menu, select *Identity Manager Integration Modules*, then click *Search*. You can narrow your search by entering Banner in the *Keyword* field.

Products

basic search | advanced search | My Restricted Downloads

Product or Technology (optional)
Identity Manager Integration Modules

-- Select Version --

All Dates

Keyword (optional)

→ search
→ clear selections

Patches
(Open and Restricted)

NOTE: Maintenance (or subscription) now required to access patches and for many Novell products.
[Read More](#)

→ search patches

products (52)

52 Results Found - 1-52 Results per page: 100 Sort By: Date

Name - click for description	File Name	Date
------------------------------	-----------	------

- 3 On the Novell Identity Manager Downloads page, click *Download* next to *Identity Manager Integration Module 4.0.1 for Banner*.
- 4 Follow the on-screen prompts to download the file to a directory on your computer.

If you haven’t already verified that the media you burned is valid, you can check it by using the *Media Check* option.

2.2 New Installation by Using Physical Media or ISO

In order to use the ISO downloaded in [Section 2.1, “Getting the .iso File from the Novell Download Site,” on page 11](#) either mount the ISO as a folder in your file system, or burn the ISO to CD or DVD and insert the disc that you created into the CD-ROM or DVD drive of the computer that you want to be your Identity Manager 4.0.1 server.

1 From ISO mount folder or the CD root folder\Additional_Drivers\SungardBanner, start the installation by executing the correct program for your workstation’s platform.

- ♦ **Windows:** If you are installing to the Identity Vault server, copy `sungardbannershim.jar` to the DirXML Drivers directory. The default value is `c:\novell\nds\lib`. If you are using the Remote Loader to run the driver, then copy `sungardbannershim.jar` to `c:\novell\remoteloader` on the machine running the Remote Loader.
- ♦ **Linux:** `rpm -ivh novell-DXMLBanner.rpm`
- ♦ **Solaris:** `pkgadd -d novell-DXMLBanner.pkg`

2 In order to use the pre-config package within Designer, you need to extend the eDirectory schema.

- ♦ **Windows:**
 1. Click *Start >Settings > Control Panel >Novell eDirectory Services .*
 2. Click *install.dim*, then click *Start*.
 3. Click *Install Additional Schema files*, then click *Next*.
 4. Log in as a user with administrative rights, then click *OK*.
 5. Specify the schema file path and name (`<InstallDirectory>\Banner.sch`).
 6. Click *Finish*.
- ♦ **Linux/UNIX:**

```
/opt/novell/eDirectory/bin/ndssch -h <localhost:524> -t <MyTreename>  
<admin_fdn> /opt/novell/eDirectory/lib/nds-schema/Banner.sch
```

3 If necessary, restart eDirectory after the driver binary and schema have been updated.

- ♦ **Windows:**

Use services to restart your eDirectory instance.
- ♦ **Linux/UNIX:**

```
/etc/init.d/nds restart
```

Creating a Working Driver

3

After the Sungard Banner driver files are installed on the server where you want to run the driver (see [Chapter 2, “Installing the Sungard Banner Driver,” on page 11](#)), you can create the driver in the Identity Vault. You do so by importing the driver configuration file and then modifying the driver configuration to suit your environment.

The following sections provide instructions to create the driver:

- ♦ [Section 3.1, “Creating the Driver in Designer,” on page 13](#)
- ♦ [Section 3.2, “Activating the Driver,” on page 22](#)
- ♦ [Section 3.3, “Sungard Banner Requirements,” on page 22](#)

3.1 Creating the Driver in Designer

You create the Sungard Banner driver by importing the driver’s configuration file and then modifying the configuration to suit your environment. After you have created and configured the driver, you need to start it.

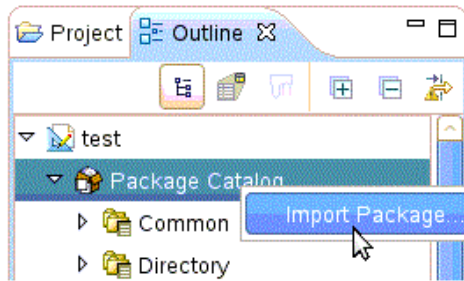
- ♦ [Section 3.1.1, “Installing the Current Driver Packages,” on page 13](#)
- ♦ [Section 3.1.2, “Installing the Driver,” on page 14](#)
- ♦ [Section 3.1.3, “Configuring the Driver,” on page 17](#)
- ♦ [Section 3.1.4, “Configuring Driver Parameters,” on page 17](#)
- ♦ [Section 3.1.5, “Deploying the Driver,” on page 18](#)
- ♦ [Section 3.1.6, “Extending the Schema,” on page 19](#)
- ♦ [Section 3.1.7, “Understanding Institutional Roles,” on page 20](#)
- ♦ [Section 3.1.8, “Starting the Driver,” on page 21](#)

3.1.1 Installing the Current Driver Packages

The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer and can be updated after they are initially installed. You must have the most current version of the packages in the Package Catalog before you can create a new driver object.

To verify that you have the most recent version of the driver packages in the Package Catalog:

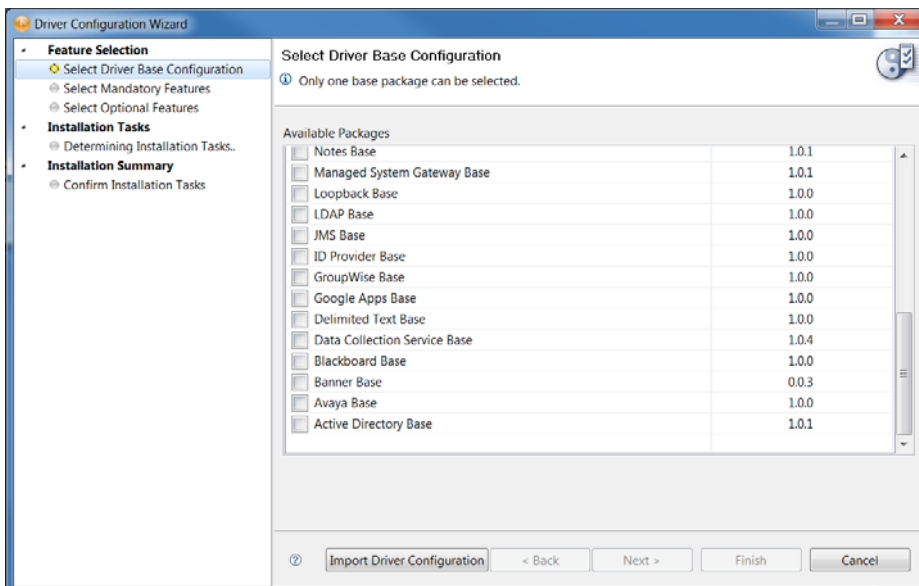
- 1 Open Designer .
- 2 In the toolbar, click *Help > Check for Package Updates*.
- 3 Click *Yes* to update the packages or click *OK* if the packages are up-to-date.
- 4 In the Outline view, right-click the Package Catalog.
- 5 Click *Import Package*.



- 6 Select any Sungard Banner driver packages
or
Click *Select All* to import all of the packages displayed.
By default, only the base packages are displayed. Deselect *Show Base Packages Only* to display all packages.
- 7 Click *OK* to import the selected packages, and then click *OK* in the successfully imported packages message.
- 8 After the current packages are imported, continue with section, [Section 3.1.2, “Installing the Driver,”](#) on page 14.

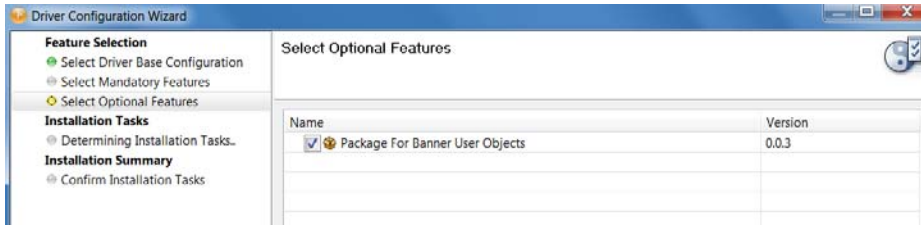
3.1.2 Installing the Driver

- 1 In Designer, open your project.
- 2 Right-click the driver-set where you want to configure the Sungard Banner driver, select *New* and then *Driver*. In the Driver Base Package Configuration screen, scroll down to find the Banner Base package. Click the box next to *Banner Base*.



- 3 Select *Banner Base*, then click *Next*.
- 4 Select the optional features to install for the Sungard Banner driver.
By default *show Only applicable package versions* is selected as expected.

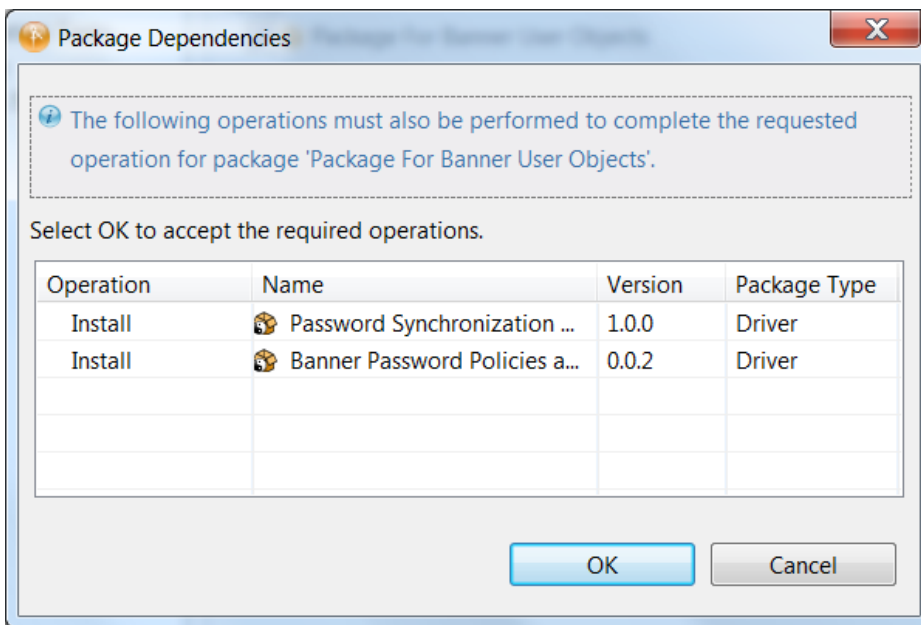
5 Select the optional Sungard Banner User Package.



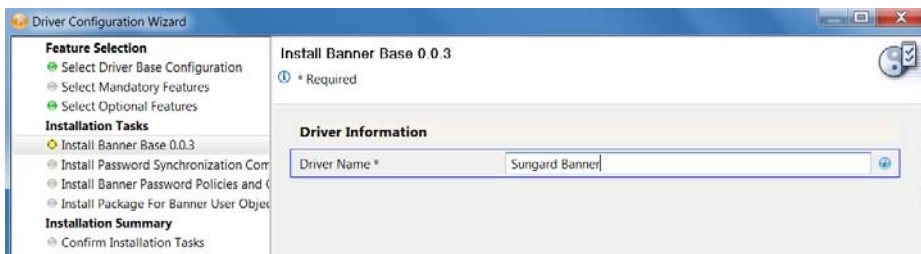
6 Click *Next*

7 (Conditional) If there are package dependencies for the packages you selected to install, you must install them to install the selected package. Click *OK* to install package dependencies.

There will be mutable instance of this; one for each option selected.



8 On the Install Sungard Banner Base page, specify a name for the driver that is unique within the driver set, then click *Next*.

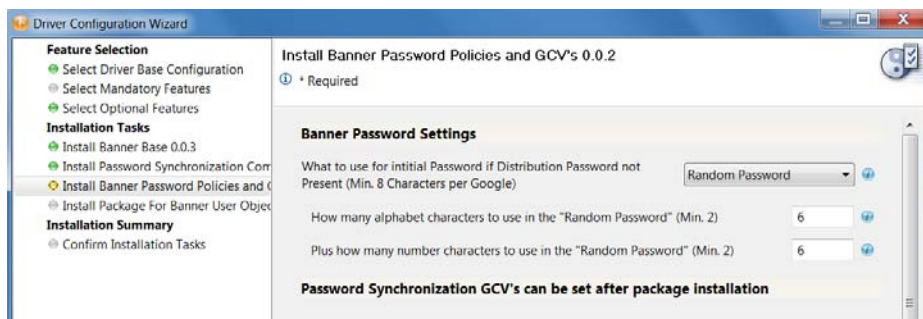


9 Set Banner Password Settings to configure how new user passwords are generated.

- ♦ Select *Random Password* to have the password policy generate a random password. Select the number of letters and the number of digit characters to be included in the password.

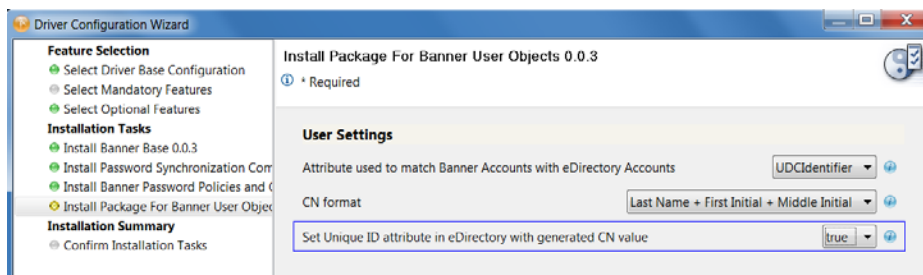
- ◆ Select *Attribute Value from User* to use the value of an attribute on the user as the password. The attribute name is selected from the eDirectory namespace.

Map a UDCIdentity attribute or BEIS extension attribute to an eDirectory attribute to support this policy. Ensure that the eDirectory attribute is entered in the driver filter as Notify to prevent the password from being written to the eDirectory attribute.



10 Configure the settings for User objects:

- ◆ **Attribute used to match Banner Users with eDirectory Users:** Select the attribute to use as the matching attribute.
 - ◆ **UDCIdentifier:** Select this UDCIdentifier to use Banner's unique object ID as the matching value.
 - ◆ **CN:** Select *CN* to use the CN as the matching attribute.
- ◆ **CN Format:** CN Format lets you select from a set of predefined patterns for constructing the new user's CN.
 - ◆ UDCIdentifier
 - ◆ First Initial + Last Name
 - ◆ First Name + Last Initial
 - ◆ First Name + Last Name
 - ◆ First Initial + Middle Initial + Last Name
 - ◆ Last Name + First Initial + Middle Initial
- ◆ **Set Unique ID attribute in eDirectory with generated CN value:** Setting this to *true* causes the generated CN value to also be stored in the Unique ID attribute.



11 Review the Summary.

12 Select *Finish*.

There is no screen during import to set authentication information. The Sungard Banner driver requires separate server and authentication information for each channel.

3.1.3 Configuring the Driver

After importing the driver configuration file, you need to configure the driver before it can run.

- ◆ There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to review [Appendix A, “Driver Properties,” on page 27](#). The Driver Parameters and the Global Configuration Values let you configure the Sungard Banner login information and security credentials, and other parameters associated with the Publisher channel. These settings must be configured properly for the driver to start and function correctly. If you do not have the Driver Properties page displayed in Designer:

- 1 Open your project.
- 2 In the Modeler, right-click the driver icon or the driver connection, then select *Properties*.
- 3 Make any desired changes, then click *OK* to save the changes.
- 4 After the driver is created in Designer, it must be deployed to the Identity Vault. Proceed to [Section 3.1.4, “Configuring Driver Parameters,” on page 17](#)

3.1.4 Configuring Driver Parameters

The *Driver Parameters* panel contains driver-specific configuration.

Driver Options

The Sungard Banner driver does not use any Driver Options. This panel is intentionally blank. Continue with [“Subscriber Options” on page 17](#)

Subscriber Options

- ◆ **URL of the remote Sungard Banner server:** Specify the IP address or URL of the BEIS listener.

`http://10.10.1.7:4041`

If you are configuring the driver to use SSL, the URL must contain a DNS name. For example:
`https://prod.bannerservice.com:4041`

- ◆ **Authentication ID:** Enter the authentication ID the driver should use when authenticating to the BEIS listener.
- ◆ **Authentication Password:** Enter the password corresponding to the authentication ID.
- ◆ **Proxy host and port:** When a proxy host and port are used, specify the host address and the host port. For example: 192.10.1.3:18180. Choose an unused port number on your server. Otherwise, leave this field blank.

After completing these configuration tasks, continue with [“Publisher Options” on page 18](#)

Publisher Options

- ♦ **Listening IP Address and Port:** Specify the IP address of the server where this driver is installed and the port that this driver listens on as an SPML Server. You can specify 127.0.0.1 if there is only one network card installed in the server. Choose an unused port number on your server. For example: 127.0.0.1:18180. The driver listens on this address for SPML requests, processes them, and returns a result.
- ♦ **Require Authentication:** Select *Show* to configure authentication information required by the Publisher channel.
- ♦ **Authentication ID:** Specify the Authentication ID to validate incoming SPML requests.
- ♦ **Authentication Password:** Specify the Authentication password to validate incoming SPML requests.
- ♦ **Accept HTTPS Connections:** Select *Yes* to enable HTTPS connections.
- ♦ **KMO Name:** When this server is configured to accept HTTPS connections, this is the KMO name in eDirectory. The KMO name is the name before the ' - ' in the RDN. Leave this field blank when a keystore file is used or when HTTPS connections are not used.
- ♦ **Keystore File:** When this server is configured to accept HTTPS connections, this is the path and the name of the keystore file. For example: C:\security\keystore. Leave this field blank when a KMO name is used or when HTTPS connections are not used.
- ♦ **Keystore Password:** When this server is configured to accept HTTPS connections, this is the keystore file password. Leave this field blank when a KMO name is used or when HTTPS connections are not used.
- ♦ **Server Key Alias:** When this server is configured to accept HTTPS connections, this is the key alias. Leave this field blank when a KMO name is used or when HTTPS connections are not used.
- ♦ **Server Key Password:** When this server is configured to accept HTTPS connections, this is the key alias password (not the keystore password). Leave this field blank when a KMO name is used (see above) or when HTTPS connections are not used.
- ♦ **Content Type:** The HTTP request header is set to this value on publisher results that are sent back to the requester.
- ♦ **Heartbeat Interval:** Specify the length of time in seconds the between heartbeats emitted by the Sungard Banner driver's Publisher channel.

After completing these configuration tasks, continue with [“Global Configuration Values \(GCVs\)” on page 18](#)

Global Configuration Values (GCVs)

The GCVs are defined in [Table A-5 on page 32](#).

After completing these configuration tasks, continue with [Section 3.1.5, “Deploying the Driver,” on page 18](#).

3.1.5 Deploying the Driver

After the driver is created in Designer, it must be deployed into the Identity Vault.

- 1 In Designer, open your project.

- 2 In the Modeler, right-click the driver icon or the driver connection, then select *Live > Deploy*.
- 3 Read through the deployment summary, and then click *Deploy*.
- 4 Read the success message, and then click *OK*.
- 5 Click *Define Security Equivalence* to assign rights to the driver.

The driver requires rights to objects within the Identity Vault. Create a user in eDirectory for the driver to use. Assign that user administrative rights to the objects that it will need to manage objects in eDirectory.

Setting the Driver object's Security Equivalence directly to the admin user is not recommended. Also, creating a new user for the driver and setting the new user object's Security Equivalence to the Admin user is not recommended. The best practice is to assign specific administrative rights as needed by the driver to a user object created for the driver.

- 5a Click *Add*, then browse to and select the object with the correct rights.
- 5b Click *OK* twice.
- 6 Click *Exclude Administrative Roles* to exclude users that should not be synchronized.
 - 6a Click *Add*, then browse to and select the user object you want to exclude.
 - 6b Click *OK*.
 - 6c Repeat [Step 6a on page 19](#) and [Step 6b on page 19](#) for each object you want to exclude.
 - 6d Click *OK*.
- 7 Click *OK*

3.1.6 Extending the Schema

Extending the schema is done to synchronize the identity information of user provisioning in Sungard HE in the existing eDirectory class `USER`, which has been modified to add the following attributes:

Attribute Name	Definition	Syntax	Type
udcMiddleName	Stores the middle initial, or part of the middle name.	CASE_IGNORE_ STRING	Single-valued attribute. 8 characters are stored for this attribute.
udcGender	Stores the gender: male, female, unknown.	CASE_IGNORE_ STRING	Single-valued attribute.
udcBirthDate	Stores the birthdate: mmddyy	CASE_IGNORE_ STRING	Single-valued attribute.
udcTaxID	Stores a number. This could be the Social Security number.	CASE_IGNORE_ STRING	Single-valued attribute.

Attribute Name	Definition	Syntax	Type
udcIdentifier	A unique key to identify the individual in the Sungard system. The driver uses this as the association key to facilitate using AccessManager to secure Sungard's Web applications.	CASE_IGNORE_ STRING	Single-valued attribute.
udcInstitutionalRoles	Role information from Sungard HE.	CASE_IGNORE_ STRING	Multi-valued attribute.
udcHomeSA	Home street address	CASE_IGNORE_ STRING	Single-valued attribute

3.1.7 Understanding Institutional Roles

- ♦ [“Role Attributes” on page 21](#)
- ♦ [“How Institutional Roles Work” on page 21](#)
- ♦ [“How Roles are Stored in udcInstitutionalRoles” on page 21](#)

Sungard provides access to applications and data by the roles applied to the people in the higher education institution. Any person might have a number of roles. For example, a university student might also be a staff member. Sungard provides 40 roles and also allows the users to add their own roles. The following list indicates some of the roles that Sungard provides:

- ♦ PROSPECTIVE
- ♦ PROSPECTIVESTUDENT
- ♦ APPLICANT
- ♦ INSTITUTIONACCEPT
- ♦ APPLICANT ACCEPT
- ♦ STUDENT
- ♦ ALUMNI
- ♦ FRIENDS
- ♦ STAFF
- ♦ DEVELOPMENTOFFICER
- ♦ FINANCE
- ♦ FACULTY
- ♦ BANNERINB

See the *Sungard HE Banner Identity Handbook* for a complete list of Sungard roles, their descriptions, and possible uses.

Role Attributes

Role	Description	
Role Name	Specifies the name of the Sungard Role.	Required
Context	The name of the Sungard component or system that created the role. Sungard always sets Context to INTCOMP.	Optional
Institution Name	If present, it identifies the institution for which this role applies.	Optional

How Institutional Roles Work

Sungard HE does not delete users from the system. Instead, roles are added to and removed from users to represent their access rights. A user with no roles has no access to Sungard applications or resources. Access to resources is based on the presence of roles. Therefore, the driver synchronizes all Role information to the `udcInstitutionalRoles` attribute in the Identity Vault. For each XML document Sungard sends to the driver Publisher channel, a complete list of the current roles on that user is provided. The driver publishes a `<remove-all-values>` command to clear the `udcInstitutionalRoles` attribute before publishing the new list of roles it received from Sungard HE.

How Roles are Stored in `udcInstitutionalRoles`

`UdcInstitutionalRoles` is a multi-valued attribute that can contain a list of roles. The three role attributes are stored in a single value, separated by semicolons. The format is: `<Role Name>;<Context>;<Institution Name>`.

Role Name is a required attribute. Context is an optional attribute. It is delimiting. A semicolon is present even if the attribute is empty. Institution Name is also an optional attribute.

For example, given a role of `BasicPerson` issued from `Banner` at `Out Of State University`, the driver generates the following:

```
<add-attr attr-name="InstitutionRoles">
  <value>BASICPERSON;Banner;OutOfStateU</value>
</add-attr>
```

3.1.8 Starting the Driver

When a driver is first created, it is stopped by default. Start the driver in order to begin synchronizing data between `Banner` and `eDirectory`. Identity Manager is an event-driven system, so after the driver is started, it waits for events to be sent from `BEIS` or `eDirectory` for processing.

To start the driver:

- 1 In Designer, select the project view.
- 2 Click the Sungard Banner driver.
- 3 Click the green start icon.

3.2 Activating the Driver

If you created the Sungard Banner driver in a driver set that has not been activated, you must activate the driver with a Sungard Banner Driver activation within 90 days. If you do not apply a Sungard Banner Driver activation within 90 days, the driver stops working.

For information on activation, refer to “[Activating Novell Identity Manager Products](#)” in the *Identity Manager 4.0 Framework Installation Guide*.

3.3 Sungard Banner Requirements

In order for the driver to interact with your Sungard Banner system, Banner Enterprise Identity Services (BEIS) needs to be configured. Configuring BEIS is outside the scope of this document.

Customizing the Driver

4

The following sections provide information to help you understand what the driver does and what customization you might need to make to the driver:

- ♦ [Section 4.1, “Managing the Driver,” on page 23](#)
- ♦ [Section 4.2, “Schema Mapping,” on page 23](#)

4.1 Managing the Driver

As you work with the Sungard Banner driver, there are a variety of management tasks you might need to perform, including the following:

- ♦ Starting, stopping, and restarting the driver
- ♦ Viewing driver version information
- ♦ Using Named Passwords to securely store passwords associated with the driver
- ♦ Monitoring the driver’s health status
- ♦ Backing up the driver
- ♦ Inspecting the driver’s cache files
- ♦ Viewing the driver’s statistics
- ♦ Using the DirXML Command Line utility to perform management tasks through scripts
- ♦ Securing the driver and its information

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *Identity Manager 4.0 Common Driver Administration Guide*.

4.2 Schema Mapping

This section details the default schema mapping of the driver. The schema map indicates how Identity Vault attributes and classes are translated into Sungard Banner attributes and classes.

The Sungard Banner driver interacts with Sungard Banner through Banner Enterprise Identity Services (BEIS). BEIS uses the UDCIdentity schema to represent user object in the Banner system. UDCIdentity is the minimal representation of a user object. It is possible to configure BEIS to include additional Banner attributes as extension attributes in the SPML documents produced by BEIS. The Banner driver processes these as <add-attr> tags, however the attribute name needs to be added to the schema map and driver filter in order to be processed through to the Identity Vault.

4.2.1 User Attributes Mapping

IDVault	Sungard Banner UDCIdentity
User	UDCIdentity
udcIdentifier	UDCIdentifier


IDVault	Sungard Banner UDCIdentity
Full Name	FormattedName
	LegalName
Given Name	GivenName
	PreferredGivenName
udcMiddleName	MiddleName
Surname	FamilyName
Generational Qualifier	Affix
udcGender	Gender
udcBirthdate	Birthdate
	Birthdate:Day
	Birthdate:Month
	Birthdate:Year
udcTaxID	TaxId
InternetEmailAddress	EmailAddress
	PrimaryAddress
co	PrimaryAddress:CountryCode
homeZipCode	PrimaryAddress:PostalCode
homeState	PrimaryAddress:Region
homeCity	PrimaryAddress:Municipality
udcHomeSA	PrimaryAddress:AddressLine
	CampusAddress
	CampusAddress:CountryCode
Postal Code	CampusAddress:PostalCode
S	CampusAddress:Region
Physical Delivery Office Name	CampusAddress:Municipality
SA	CampusAddress:AddressLine
Telephone Number	CampusPhone
	CampusPhone:InternationalCountryCode
	CampusPhone:NationalNumber
	CampusPhone:AreaCityCode
	CampusPhone:SubscriberNumber

IDVault	Sungard Banner UDCIdentity
	CampusPhone:Extension
mobile	MobilePhone
	MobilePhone:InternationalCountryCode
	MobilePhone:NationalNumber
	MobilePhone:AreaCityCode
	MobilePhone:SubscriberNumber
	MobilePhone:Extension
Fascimile Telephone Number	Fax
	Fax:InternationalCountryCode
	Fax:NationalNumber
	Fax:AreaCityCode
	Fax:SubscriberNumber
	Fax:Extension
udcInstitutionalRoles	InstitutionRoles

Driver Properties

A


This section provides information about the Driver Configuration and Global Configuration Values properties for the Sungard Banner driver. These are the only unique properties for drivers. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to “[Driver Properties](#)” in the *Identity Manager 4.0 Common Driver Administration Guide* for information about the common properties.

The information is presented from the viewpoint of iManager. If a field is different in Designer, it is marked with an  icon.

- ♦ [Section A.1, “Driver Configuration,” on page 27](#)
- ♦ [Section A.2, “Global Configuration Values,” on page 31](#)
- ♦ [Section A.3, “Extension Attributes,” on page 33](#)

A.1 Driver Configuration

In iManager:

- 1 Click  to display the Identity Manager Administration page.
- 2 Open the driver set that contains the driver whose properties you want to edit:
 - 2a In the *Administration* list, click *Identity Manager Overview*.
 - 2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.
- 3 Locate the driver icon, then click the upper right corner of the driver icon to display the *Actions* menu.
- 4 Click *Edit Properties* to display the driver’s properties page.

By default, the Driver Configuration page is displayed.

In Designer:



- 1 Open a project in the Modeler.
- 2 Right-click the driver icon or line, then select click *Properties > Driver Configuration*.

The Driver Configuration options are divided into the following sections:

A.1.1 Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.

Table A-1

Option	Description
<i>Java</i>	Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the <code>classes</code> directory as a class file, or in the <code>lib</code> directory as a <code>.jar</code> file. If this option is selected, the driver is running locally. The Java class name is: <code>com.novell.nds.dirxml.driver.sungardbannershim.SungardBannerDriverShim</code>
<i>Native</i>	This option is not used with the Sungard Banner driver.
<i>Connect to Remote Loader</i>	Used when the driver is connecting remotely to the connected system. Designer includes two suboptions: <ul style="list-style-type: none">◆  <i>Driver Object Password</i>: Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.◆  <i>Remote Loader Client Configuration for Documentation</i>: Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.

A.1.2 Driver Object Password


Table A-2

Option	Description
<i>Driver Object Password</i>	Use this option to set a password for the driver object. If you are using the Remote Loader, you must enter a password on this page or the remote driver does not run. This password is used by the Remote Loader to authenticate itself to the remote driver shim.

A.1.3 Authentication

The authentication section stores the information required to authenticate to the connected system.

Table A-3

Option	Description
<i>Authentication ID</i> or  <i>User ID</i>	The Sungard Banner driver uses separate authentication configurations for each channel. The driver does not use this Authentication information. Leave it blank.


Option	Description
<p><i>Authentication Context</i></p> <p>or</p> <p> <i>Connection Information</i></p>	<p>The Sungard Banner driver uses separate authentications for each channel. Leave this parameter blank.</p>
<p><i>Remote Loader Connection Parameters</i></p> <p>or</p> <p> <i>Host name</i></p> <p> <i>Port</i></p> <p> <i>KMO</i></p> <p> <i>Other parameters</i></p>	<p>Used only if the driver is connecting to the application through the remote loader. The parameter to enter is <code>hostname=xxx.xxx.xxx.xxx port=xxxx</code> <code>kmo=certificatename</code>, when the host name is the IP address of the application server running the Remote Loader server and the port is the port the remote loader is listening on. The default port for the Remote Loader is 8090.</p> <p>The <code>kmo</code> entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine.</p> <p>Example: <code>hostname=10.0.0.1 port=8090</code> <code>kmo=IDMCertificate</code></p>
<p><i>Driver Cache Limit (kilobytes)</i></p> <p>or</p> <p> <i>Cache limit (KB)</i></p>	<p>Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited.</p> <p> Click <i>Unlimited</i> to set the file size to unlimited in Designer.</p>
<p><i>Application Password</i></p> <p>or</p> <p> <i>Set Password</i></p>	<p>This option is not used with the Sungard Banner driver.</p>
<p><i>Remote Loader Password</i></p> <p>or</p> <p> <i>Set Password</i></p>	<p>Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.</p>

A.1.4 Startup Option

The Startup Option section allows you to set the driver state when the Identity Manager server is started.

Table A-4

Option	Description
<i>Auto start</i>	The driver starts every time the Identity Manager server is started.
<i>Manual</i>	The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.
<i>Disabled</i>	The driver has a cache file that stores all of the events. When the driver is set to Disabled, this file is deleted and no new events are stored in the file until the driver state is changed to Manual or Auto Start.

Option	Description
 <i>Do not automatically synchronize the driver</i>	This option only applies if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

A.1.5 Driver Parameters

The Driver Parameters section allows you to configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment. For example, you might find the default Publisher polling interval to be shorter than your synchronization requires. Making the interval longer could improve network performance while still maintaining appropriate synchronization.

Option	Description
<i>Driver Name</i>	The name of the driver contained in the driver configuration file is <code>Sungard Banner</code> . Specify the actual name you want to use for the driver.
<i>Driver is Local or Remote</i>	Configure the driver for use with the Remote Loader service or daemon by selecting <i>Remote</i> , or select <i>Local</i> to configure the driver for local use. If <i>Local</i> is selected, the remaining prompts are not displayed.
<i>Driver Password</i>	For remote driver configuration only. The driver object password is used by the Remote Loader to authenticate to the Identity Manager server. It must be the same password that is specified in the <i>Driver Object Password</i> field on the Identity Manager Remote Loader.
<i>URL of the Remote Sungard Banner Server</i>	Specify the URL for the remote Sungard Banner server.
<i>Authentication ID</i>	Specify the authentication ID for the remote Sungard Banner server.
<i>Authentication Password</i>	Specify the authentication password for the remote Sungard Banner server.
<i>Proxy Host and Port</i>	Specify the host address and the host port when a proxy host and port are used.
<i>HTTP Errors to Retry</i>	List the HTTP error codes that should return a retry status.
Customize HTTP Request-Header Fields	Select <i>Show</i> if you want to set mutual authentication information.
<i>Listening IP Address and Port</i>	Specify the IP address of the server where this driver is installed and the port number this driver listens on as an SPML server.
<i>Require Authentication</i>	The <i>basic</i> authentication scheme requires a user-ID and password.


Option	Description
<i>Authentication ID for incoming SPML requests</i>	Specify the authentication ID to validate incoming SPML requests.
<i>Authentication Password for incoming SPML requests</i>	Specify the authentication password to validate incoming SPML requests.
<i>Accept HTTPS Connections</i>	Indicates if the driver accepts HTTPS connections from Sungard Banner.
<i>KMO Name</i>	When the server is configured to accept HTTPS connections, this is the KMO name in eDirectory.
<i>Keystore File</i>	When the server is configured to accept HTTPS connections, this is the path and name of the keystore file.
<i>Keystore Password</i>	When the server is configured to accept HTTPS connections, this is the keystore file password.
<i>Server Key Alias</i>	When the server is configured to accept HTTPS connections, this is the key alias.
<i>Server Key Password</i>	When the server is configured to accept HTTPS connections, this is the key alias password, not the keystore password.
<i>Content-Type</i>	The HTTP request header is set to this value on publisher results that are sent back to the requester.
<i>Heartbeat Interval in Minutes</i>	Specify the heartbeat interval in minutes.

A.2 Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The Sungard Banner driver includes several predefined GCVs. You can also add your own if you discover you need additional ones as you implement policies in the driver.

To access the driver's GCVs in iManager:

- 1** Click  to display the Identity Manager Administration page.
- 2** Open the driver set that contains the driver whose properties you want to edit:
 - 2a** In the *Administration* list, click *Identity Manager Overview*.
 - 2b** If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c** Click the driver set to open the Driver Set Overview page.
- 3** Locate the driver icon, click the upper right corner of the driver icon to display the *Actions* menu, then click *Edit Properties*.

or

To add a GCV to the driver set, click *Driver Set*, then click *Edit Driver Set properties*.

To access the driver's GCVs in Designer:



- 1 Open a project in the Modeler.
 - 2 Right-click the driver icon  or line, then select *Properties > Global Configuration Values*.
- or
- To add a GCV to the driver set, right-click the driver set icon , then click *Properties > GCVs*.

Table A-5

Name	Description	Example Value
Banner Password Settings		
What to use for initial Password if Distribution Password not Present	If the system is not set up for universal password synchronization or the user account doesn't have a distribution password set yet, then an initial password must be set. This GCV tells the system whether to use an attribute from the user account for an initial password or to use a randomly generated password. If the accounts will use SAML for authentication, then you can use a random password. Otherwise, select an attribute value.	<i>Random Password or Attribute Value from User</i> <hr/> NOTE: The attribute name must be specified in eDirectory namespace. The Banner attribute that contains the password value needs to be mapped to the eDirectory attribute name. The attribute should be marked as Notify in the driver filter to prevent the password value from being written to eDirectory.
eDirectory attribute to use for initial password value.	The name of the attribute in eDirectory that the Sungard Banner driver should use for an initial password if no Distribution password is available on creation.	Surname
Number of letters to use in the Random Password	The number of alphabetic characters to use in the random password. When this number is added to the value of the Random Password Numbers GCV, it determines the number of characters in the total length.	6
Number of numbers to use in the Random Password	This is the number of numbers to use in the random password. when added to the value of the "Random password letters" GCV It will determine the number of characters in the total Length.	6
User Settings		
Attribute used to match Banner users to eDirectory users.	This GCV allows selection of the attribute used by the driver's matching policy.	<i>UDCIdentifier</i> causes the matching rule to match objects using the UDCIdentifier. This is a unique ID generated by Banner <i>CN</i> causes the matching rule to use the CN

Name	Description	Example Value
CN Format	This GCV contains a set of patterns that can be used to generate a new user's CN	<ul style="list-style-type: none"> ◆ UDCIdentifier ◆ First Initial + Last Name ◆ First Name + Last Initial ◆ First Name + Last Name ◆ First Initial + Middle Initial + Last Name ◆ Last Name + First Initial + Middle Initial
Set Unique ID attribute in eDirectory with generated CN value	If this is set to <i>true</i> , then the CN value for new users is copied to the eDirectory Unique ID attribute	<i>true</i> or <i>false</i>

A.3 Extension Attributes

BEIS is configured to publish objects based on the UDCIdentity schema. All attributes of the UDCIdentity that are present on the user are published in the SPML document. Additionally, BEIS can be configured to publish other Banner attributes on Banner user objects.

The Banner driver publishes extension attributes like any other UDCIdentity schema element.

For example, if there is a Banner extension attribute named GORMAL_EMAIL_ADDRESS with a value of bob@outofstate.edu, the driver generates the following:

```
<add-attr attr-name="GOREMAL_EMAIL_ADDRESS">
  <value>bob@outofstate.edu</value>
</add-attr>
```

Because the driver only reports UDCIdentity attributes in response to a schema request, extension attributes don't show up by default in the schema map. They need to be added by hand. In a future release, the driver will "learn" about extensions and report them when the schema is requested.

Securing the Driver

B

Banner Enterprise Identity Services (BEIS) can be configured to use SSL. You can configure the driver to accept HTTPS connections and take advantage of this increased security.

IMPORTANT: Only certificates from a Java keystore are accepted. Make sure that the keystore for the certificates is a Java keystore.

The following sections provide instructions for creating a secure connection:

- ♦ [Section B.1, “Configuring the Publisher Channel,” on page 35](#)
- ♦ [Section B.2, “Configuring the Subscriber Channel,” on page 36](#)

B.1 Configuring the Publisher Channel

- 1 Create a server certificate using keytool.

For more information on keytool, see [Keytool - Key and Certificate Management Tool \(http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html\)](http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html)

```
. keytool -genkey -keyalg RSA -alias selfsigned -keystore  
key_store_file_name -storepass password -validity 360 -keysize 2048
```

For example: `keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore.jks -storepass changeit -validity 360 -keysize 2048`

You are prompted for the following information:

- ♦ **What is your first and last name?**
This becomes the CN of your certificate. Specify the DNS name of the server running the driver.
- ♦ **What is the name of your organizational unit?**
Specify the name of your organizational unit. This information does not need to correlate to any information in eDirectory or DNS.
- ♦ **What is the name of your organization?**
Specify the name of your organization. This information does not need to correlate to any information in eDirectory or DNS.
- ♦ **What is the name of your city or locality?**
Specify the name of your city. This information does not need to correlate to any information in eDirectory or DNS.
- ♦ **What is the name of your state or province?**
Specify the name of your state. This information does not need to correlate to any information in eDirectory or DNS.
- ♦ **What is the two-letter country code for this unit?**
Specify the code for your country. This information does not need to correlate to any information in eDirectory or DNS.

keytool will present a summary of your information and asks if it is correct. Press Y.

- 2 Configure the Publisher channel to use the server certificate created in [Step 1 on page 35](#)
 - 2a In Designer, right-click on the driver and select *Properties*.
 - 2b In the Properties dialog box, select *Driver Configuration*
 - 2c For Driver Configuration, select the *Driver Parameters* tab.
 - 2d On the *Driver Parameters* tab, select *Publisher Options* tab.
 - 2e For *Accept HTTPS Connections* select *Yes*.
 - 2f Specify the path and filename of the keystore you created in [Step 1 on page 35](#). For example, enter `c:\keystore.jks`.
 - 2g Specify the password of the keystore you created in [Step 1 on page 35](#). For example, enter `changeit`.
 - 2h Specify the server key alias of the key you created in [Step 1 on page 35](#). For example, enter `selfsigned`.
 - 2i Enter the password for the server certificate you created in [Step 1 on page 35](#). For example, enter `changeit`.
- 3 Click *OK* to save your changes.

B.2 Configuring the Subscriber Channel

The Subscriber channel sends information from the Identity Vault to Banner via Banner Enterprise Identity Services. To establish a secure connection you need a trust store containing a certificate issued by the certificate authority that signed the BEIS server certificate. You need to obtain this certificate from a BEIS administrator.

- 1 Make sure you have a certificate signed by the certificate authority from the BEIS administrator.
- 2 Import the certificate into your trust store, or create a new trust store by entering the following command at the command prompt: `keytool -import - file name_of_cert_file - trustcacerts -noprompt -keystore filename -storepass password`
 For example: `keytool -import - file beis_cert.b64 -trustcacerts -noprompt - keystore dirxml.keystore -storepass changeit`
 For more information on keytool, see [Keytool - Key and Certificate Management Tool \(http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html\)](http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html)
- 3 Configure the Subscriber Channel to use the trust store created in [Step 2](#)
 - 3a In iManager, in the *Roles and Tasks* view, click *Identity Manager > Identity Manager Overview*.
 - 3b Locate the driver set containing the Sungard Banner Driver. Then click the driver's icon to display the Identity Manager Driver Overview page.
 - 3c On the Identity Manager Driver Overview page, click the driver's icon again and then scroll to *Subscriber Settings*.
 - 3d In the *Keystore File* setting, specify the path to the trust store you created in [Step 2](#).
- 4 Click *Apply*, then click *OK*.